



## **COMPLIANCE POLICY**

**DUNAMIS TRADING GESTÃO DE  
RECURSOS LTDA**

**June 2024**



## Summary

<b>1. INTRODUCTION</b>	<b>2</b>
<b>2. REGULATORY ENVIRONMENT</b>	<b>2</b>
<b>3. ROLES AND RESPONSIBILITIES</b>	<b>3</b>
<b>4. SANCTIONS</b>	<b>6</b>
<b>5. CONFIDENTIALITY POLICY</b>	<b>6</b>
5.1 CONFIDENTIAL INFORMATION MANAGEMENT	7
5.2 INSIDER TRADING AND “CLUES”	8
5.3 FRONT-RUNNING	9
<b>6. ACTIVITIES SEGREGATION AND MISALIGNMENT MONITORING POLICY</b>	<b>9</b>
6.1. ACTIVITIES SEGREGATION	9
6.2 MISALIGNMENT MONITORING	10
<b>7. CONFLICT OF INTERESTS</b>	<b>11</b>
<b>8. PARTY POLITICS</b>	<b>11</b>
<b>9. TRAINING POLICY</b>	<b>12</b>
<b>10. INFORMATION SECURITY</b>	<b>12</b>
<b>11. MONITORING AND ACCESS CONTROL</b>	<b>14</b>
<b>12. INFORMATION ARCHIVING</b>	<b>15</b>
<b>13. ANTI-MONEY LAUNDERING POLICY AND KNOW YOUR CLIENT (“KYC”)</b>	<b>15</b>
13.1. MONEY LAUNDERING	15
13.2. COAF COMMUNICATION	16
13.3. KNOW YOUR CLIENT	17
<b>14. ANTICORRUPTION POLICY</b>	<b>17</b>
<b>15. ADVANTAGES, BENEFITS AND GIFTS</b>	<b>18</b>
<b>16. SOFT DOLLAR</b>	<b>18</b>
<b>17. THIRD PARTY HIRING POLICY</b>	<b>20</b>
17.1. PROCEDURES	20
17.2. BROKERS HIRING	20
17.3. BACK-OFFICE HIRING	21
<b>APPENDIX I - ENGAGEMENT LETTER</b>	<b>22</b>
<b>APPENDIX II - CONFIDENTIALITY AGREEMENT</b>	<b>24</b>
<b>APPENDIX III - MAIN REGULATIONS</b>	<b>27</b>



## 1. Introduction

This Compliance Policy (“Policy”) was prepared based on the provisions in item 2.7 of Circular Memorandum/CVM/SIN/No. 05/2014 and CVM Instruction No. 558/15 (Brazilian Securities and Markets Commission - CVM Instruction No. 558), in order to establish, jointly with the Ethics Code, principles, concepts and values that guide the conduct of all those who hold a position, function, post, corporate, employment, commercial, professional, contractual or trust relationship (“Employees”) at **DUNAMIS TRADING GESTÃO DE RECURSOS LTDA.** (“Manager”), both in its internal performance and in communication with different audiences.

The Manager's objective is investment funds and securities portfolios management of its own and third parties, focusing on multimarket investment funds, shares, and securities, in Brazil and abroad.

The Manager does not intend to carry out activities other than the asset management activity described in its Articles of Association and, therefore, it will not be subject to the rules for consulting and distribution of securities established in the applicable regulations, notably in CVM 558.

The Manager and its Employees do not admit and repudiate any manifestation of prejudice related to origin, race, religion, social class, gender, physical disability, or any other form of prejudice that may exist.

In case of doubts or need for advice on the rules contained in this manual, it is essential that the Employee seek immediate assistance from any of the Compliance Committee members or the Compliance Officer (as defined below).

The Manager shall prepare and maintain updated versions of this Policy on its website <http://www.dunamistg.com> and/or <http://www.dunamistrading.io>, along with the following documents: (i) Reference Form, the contents of which shall reflect Appendix 15-II of CVM Instruction 558; (ii) Ethics Code; (iii) Personal Investment Policy; (iv) Risk Management Policy; and (v) Securities Portfolios Orders Proration and Division Policy.

## 2. Regulatory Environment

This Policy is an integral part of the rules governing corporate or employment relationship of the Employees, who, by signing the Engagement Letter contained in Appendix I of this Policy (“Engagement Letter”), expressly accept the principles set forth herein.

When signing the Engagement Letter, each Employee undertakes to ensure the application of



Compliance rules and principles contained in this Policy. Periodically, Employees may be required to sign new Engagement Letters, reinforcing their knowledge and agreement with the terms of this Policy.

In addition, all Employees must ensure a perfect understanding of the laws and regulations applicable to the Manager (the main ones being transcribed in Appendix III of this Code), as well as the complete content of this Policy.

In the event of having a suspicious situation with conflict potential or occurrence action that may affect the interests of the Manager, the Employee must follow this same guidance. This is the most transparent and objective way to consolidate the values of the Manager's corporate culture and reinforce its ethical principles.

Non-compliance, suspicion, or evidence of non-compliance with any of the rules established in this Policy or the other rules applicable to the Manager's activities must be brought to the appreciation of the Manager's administrators, in accordance with the procedures set out in this Policy. The Compliance Committee will be responsible for determining and applying, through any of its members, the sanctions resulting from such deviations, under the terms of this Code, guaranteeing the Employee ample right of defense.

It is every Employee's duty to inform any Compliance Committee member about violations or suspicions, indications of possible violations of the principles and rules set forth herein by other Employees, including information or situations in progress that may generate conflicts or affect the Manager's interests, to preserve the Manager and its clients' interests, as well as to care for the company's reputation. In case of violation or suspected violation falls on any of the members of the Compliance Committee, the Employee must report directly to any other member of this Committee.

Violation of any of the rules described herein, in addition to those contained in this Policy's Appendixes and other rules applicable to the Manager's activities, will be considered a contractual infraction, subjecting the author to the applicable penalties. The Manager does not assume the responsibility of Employees who violate the law or commit violations in the performance of their duties. Should the Manager be held liable or suffer losses of any nature due to the actions of its Employees, it may exercise the right of recourse in the face of those responsible, under the terms of the applicable legislation in force.

### **3. Roles and Responsibilities**

The Compliance Officer is the officer responsible for the implementation and fulfillment of the Manager's rules, procedures and internal controls, of CVM Instruction 558/15.

In carrying out the activities under his responsibility, established in or out of this Policy, the Compliance Officer may use electronic systems and/or lawyers services or *Compliance* consulting



firms for support and assistance in his functions.

It will be up to the Compliance Officer, without prejudice to other activities attributed to him:

- a) to establish the Compliance Policies, the content of the Ethics Code and other institutional policies that concern compliance in conducting business, in order to avoid violations and misconduct; in this sense, internal policies are transmitted to new employees, with the completion and signing of an engagement letter requested for each of these policies and filed at the company. When the content is updated, new versions of the policies are transmitted by email to all Employees;
- b) to assist advising the Manager in decision-making processes necessary for implementing institutional strategies, actively and continuously following the values and beliefs transmitted and incorporated by the Manager's Employees;
- c) to continuously monitor the regulatory environment and its changes, making sure that they adhere to the laws, regulations and rules published by regulatory organs and supervisory bodies, in addition to observing the best market practices established by class associations and the self-regulatory body;
- d) to validate the products negotiated and services provided by the Manager, from the *Compliance* perspective, that is, ensuring their compliance with the set of laws and rules that govern these activities, as well as assessing their vulnerability to money laundering and other criminal activities;
- e) to disseminate a money laundering and financing of terrorism prevention culture through specific policies and procedures and the preparation of periodic face-to-face training programs, as determined by regulatory bodies;
- f) to create mechanisms to know, evaluate and monitor, according to current regulations, customers, employees or suppliers that fit as a Politically Exposed Person - PEP;
- g) to provide communication channels to encourage suspicious operations and situations reporting, in accordance with institutional policies and requirements in force by regulatory bodies;
- h) to prevent image risk of the Manager by ensuring that the financial resources used in the operations are of lawful origin;
- i) to maintain relations with regulatory bodies, trade associations and important market participants and assist them in their claims for information and reports, and be involved in making decisions related to the area;
- j) to evaluate, within the scope of the Compliance Committee, any acts that may characterize, directly or indirectly, a failure by Employees to comply with the provisions of this Policy, Ethics Code and Manager's other policies;
- k) to define procedures to be adopted to repress acts practiced in disagreement with the policies adopted by the Manager, as well as to establish penalties or mechanisms to repair the damages suffered by the same or third parties due to this non-compliance;
- l) to proceed with the Employee training and retraining program, which will be carried out at least annually or as the rules and principles contained in the Compliance Policy and the Ethics Code are updated, aiming to ensure that they are always up to date, participation is obliged to all in such retraining programs; in this sense, internal manuals are transmitted to



new employees or those undergoing retraining, with the completion and signing of an engagement letter requested for each of these trainings, and filed at the company. When content is updated, new versions of the manuals are transmitted by email to all Employees;

- m) to annually prepare an internal report on internal controls and compliance, as established in article 22 of CVM Instruction 558, which must be made available to the Compliance Committee and Executive Partners, containing:

I - The conclusions of the tests carried out and, in the appendix, the list of the Compliance area internal controls.

II - The recommendations regarding possible deficiencies, with the establishment of sanitation schedules, when applicable; and

III - the statement of the responsible officer for securities portfolios management or, when applicable, the responsible officer for risk management regarding deficiencies found in previous verifications and planned measures, according to specific schedule, or effectively adopted to remedy them.

Employees who are aware of information or situations in progress that may affect the Manager's interests, generate conflicts or, even if they prove to be contrary or potentially contrary to the terms provided for in this Policy, shall promptly inform any of the Compliance Committee members.

The Compliance Committee will be composed of the Compliance Officer, the Investment Officer and the Risk Officer. The meetings are held at least every six months and their resolutions are recorded in minutes or email.

It will be up to the Manager's Compliance Committee and its members, with respect to Compliance activity, as applicable, related to this Policy:

- a) to define the ethical principles to be observed by all Manager's Employees provided herein this Policy or in other documents that may be produced for this purpose, preparing its periodic review;
- b) to analyze and discuss situations that come to your knowledge that can be characterized as personal and professional "conflicts of interest";
- c) to promote the wide dissemination and application of ethical precepts in the development of all the Manager's Employees activities;
- d) to evaluate all cases that come to your knowledge about potential non-compliance with ethical and *Compliance* provisions provided for in this Policy or in the other documents mentioned here, and evaluate and analyze unforeseen situations;
- e) to ensure information confidentiality on any crimes or offenses, even when not request so, except in the event of a legal testimony;
- f) to request, when necessary, for the analysis of his/her questions, the support of internal or external audit or other professional advisers;
- g) to treat all matters that come to his/her attention as confidential and preserve the Manager's institutional and corporate interests and image, as well as all Employees involved;



- h) to define and to apply eventual sanctions to Employees, beyond analyzing eventual cases of infraction of the described rules in the Manager's Ethics Code and Compliance Policy or other significant events.

Notwithstanding, in case that the deliberate subject involves the analysis of non-compliance, suspicion, or indication of non-compliance of any of the rules provided in the Policy or other applicable rules to the Manager's activities for any of the Compliance Committee members, the respective involved member will be hindered to vote on such questions, without damage to a ample right of defense.

In accord with the previous paragraph, the Compliance Committee will establish the eventual sanctions to be applied, if the case, in accordance with the procedures established in the Policy, being that same in this scope, in case that the subject involves any of its members, this member will remain hindered to vote.

#### **4. Sanctions**

The sanctions arising from non-compliance with the principles set forth in this Policy by the Manager's Employees are to be defined and applied by the Compliance Committee, insuring to the Employee ample right to defense. Warning penalties, suspension, termination, or discharge for cause may apply, among other penalties, where applicable, in the event of the Employees are Manager's partners, in this last case, in accordance with article 482 of The Brazilian Labor Law, without prejudice to the right of the Manager to claim damages for any incurred losses, damages or harm and/or loss of profits, by means of appropriate legal measures.

The Manager does not assume the responsibility of Employees who violate the law or commit violations in the performance of their duties. Should the Manager be held liable or suffer losses of any nature due to the actions of its Employees, it may exercise the right of recourse in the face of those responsible.

The Employee who has knowledge of or suspicion of non-compliance act with the devices of this Policy, must report, immediately, such event to any of the Compliance Committee members. if The Employee omits such obligation, he/she might suffer disciplinary action, discharge for cause, as the applicable legal regimen of his/her position.

#### **5. Confidentiality Policy**

The present Chapter provisions if apply the Employees who, by means of its functions in the Manager, may have or come to have access the confidential information or privileged information of financial, technical, commercial, strategical, business or economic nature, amongst others.

As provided in the Confidentiality Agreement present in Appendix II, it is strictly forbidden the disclosure of any confidential information out of the scope of the Manager's activities. It is



forbidden any disclosure, in a personal or professional sphere, that is not in accordance with legal rules (specially, but not limited to, those delineated in Appendix III of this Policy) and *compliance* with the Manager.

Are considered confidential information (“Confidential Information”), for the purposes of this Policy, regardless of this information being stored in disks, floppy discs, flash-drives, tapes, emails, other kinds of medium or physical documents, or being written, verbal or presented in a tangible or intangible manner, any information about the Manager, about the companies belonging to its conglomerate, its partners and clients, including:

- a) know-how, techniques, copies, diagrams, models, samples, computer software and network infrastructure;
- b) technical, financial, or related information to investment and divestment strategies or trading; including balances, bank statements and clients’ investment funds and portfolios positions managed by the Manager;
- c) structured operations, other operations and their respective values, analyzed or performed by investment funds and portfolios managed by the Manager;
- d) reports, studies, internal opinions on financial assets;
- e) clients list, commercial counterparts, suppliers and service providers;
- f) strategic or market information, or of any nature related to the Manager’s and its clients or partners activities;
- g) information regarding financial results previous to publication of balances, trial balances and/or financial statements of the investment funds and portfolios managed by the Manager;
- h) transactions performed and which have not yet been published; and
- i) other information obtained with Manager’s partners, officers, employees, trainees, interns or “young apprentices”, or yet, with their representatives, consultants, advisors, clients, suppliers and service providers in general.

Regarding confidentiality and information treatment, the Employee must comply with what is stated in the terms below:

### **5.1 Confidential Information Management**

The Manager, its clients and stakeholders business and its Partners and Employees personal information are strictly confidential and must not be publicized – internally or externally – in disagreement of procedures provided herein. Confidentiality it’s a component key to “Information Barriers” but must not be confused as the later. The barriers are related to the information flow. Therefore, confidential information must prevail in all areas and companies and its publicizing must follow information need principle to perform its activities (“Need To Know Basis”). Its definition precedes the information flow itself. Definitions: confidential documents/information must be classified according with the definition bellow:





<b><u>Confidential</u></b>	Documents and information that must circulate only among company's Partners in general, including personal information as defined in LGPD scope;
<b><u>Restrict</u></b>	Documents and information that must circulate only among internal departments, which need that information to perform its activities and conduct business, as well as Manager service providers or its managed funds.
<b><u>Internal</u></b>	Documents or information of internal exclusive use, involving Manager's Partners and Employees, that must only circulate within the company, external circulation is forbidden.
<b><u>Public</u></b>	Public documents and information of free circulation.

## 5.2 Insider Trading and "Clues"

*Insider Trading* means to buy and sell shares or stocks based on the use of privileged information, with the purpose of acquiring gain for oneself or third parties (included the Manager's Employees).

"Clue" is the transmission, to any third party, stranger to the activities of the Manager, of privileged information that might be used with profit in the purchase and sale of securities.

Any Employee that might possess privileged information on the terms above shall communicate to any of the members of the Compliance Committee within 48 (forty-eight) hours of the moment on which had knowledge of the information, so that the Committee takes the appropriate measures to restrain, as the case requires, the negotiation of the securities related to the privileged information.

For this Policy's purpose, it is considered privileged information any relevant information concerning any company, that has not been publicized and that is obtained in a privileged manner (due to the professional or personal relationship kept with a client, with persons related to the analyzed or invested companies, or with third parties).

Privileged information shall be maintained in secrecy by all those that had access to it, be it due to the exercise of professional activity or of personal relationship.

Employee who has access to a privileged information shall report it immediately to one of the Compliance Committee members, who shall forward the matter to the other Compliance Committee members, not divulging it to anyone, not even the other Employees, market



professionals, friends, and relatives, nor utilize it, be it on their own benefit or of third parties.

In case of doubt about the privileged character of the information, the Employee that has had access to it shall immediately report such incident to one of the Compliance Committee members, who shall forward the matter to the other Compliance Committee members. All those Employees that have access to a privileged information shall, also, totally restrict the circulation of documents and files that contain such information.

### **5.3 Front-running**

*Front-running* means the practice that involves taking advantage of any privileged information to perform or conclude an operation ahead of others.

What is stipulated in the “*Confidential Information Management*”, “*Insider Trading and Clues*” and “*Front Running*” items shall be observed not only during the extent of their professional relationship with the Manager but including after its conclusion.

The Manager’s Employees shall keep secrecy over any relevant information to which they have privileged access, until it is publicized to the market, as well as to guard so that subordinates and third parties they trust also do it, answering for the damages caused in case of non-compliance.

In case Employees have access, by any means, to privileged information, they shall take such circumstance to the immediate knowledge of any of the Compliance Committee members, indicating, beyond that, the source of the privileged information thus obtained.

Such duty of communication will also be applicable in the cases on which the privileged information is known in an accidental manner, in virtue of casual comments or by negligence or indiscretion of persons with confidentiality duty. The Employees that by these means have access to privileged information, shall abstain from making any use of or communicating it to third parties, except regarding communication to any of the Compliance Committee members as above mentioned.

It is expressly forbidden to make use of the practices above described to obtain, for oneself or others, undue advantage through negotiation, under their own name or of third parties, of securities, subjecting the Employee to the penalties described in this Policy and in the applicable legislation, including possible discharge for cause.

## **6. Activities Segregation and Misalignment Monitoring Policy**

### **6.1. Activities Segregation**



The Manager will perform activities aimed at securities portfolios managing, which are authorized and exercised by the terms of clause II of §1º of Article 2<sup>nd</sup> of CVM Instruction 558.

The activities carried out by the Manager are exhaustively regulated, especially by the Brazilian Securities and Markets Commission (“CVM”) and consist exclusively of its clients’ securities portfolios management and investment funds management, not having the need, therefore, of activities segregation.

Each and every information and/or data of confidential nature (including, without limitation, all the technical, financial, operational and economic information, as well as any other commercial information) relating to the Manager, its activities and its clients and any copies or register of these, oral or written, contained in any physical or electronic medium, that may have been directly or indirectly given or disclosed by virtue of the activity of securities portfolios management performed by the Manager, shall not be disclosed to third parties (including possible back-office and securities analysis service providers) without the previous and express consent of the Compliance Committee members.

However, the Manager will hire, at any moment, third parties that are not related to its main activity.

In this regard, all Employees shall respect the rules and segregation established in this Policy and keep the strictest and absolute secrecy regarding any information that they may have access to as a consequence of the exercise of their activities. For that purpose, each Employee, by signing the Engagement Letter, annexed to this, expressly attests that is in accordance with the rules herein established and, by signing the Confidentiality Agreement, abstains from disclosing confidential information that may have access to.

The Manager must exercise its activities with loyalty and good faith in relation to its clients, avoiding practices that might impair the fiduciary relation kept with them.

## **6.2 Misalignment Monitoring**

The Manager’s activity is regulated and monitored by regulatory and self-regulatory bodies; therefore, laws and rules establish operating rules and limits, providing several specific limits related to the diverse securities that might be acquired by a managed portfolio or an investment fund.

Thus, the Manager adopts diverse limit control systems and operational maximum percentage that have as an objective to minimize the possibility of occurring the active misalignment of the positions held.

The Manager monitors, by proprietary worksheets, the alignment of the investment funds and portfolios under its management to the legal and regulatory limits applicable to them, previously



to the execution of operations.

However, occasionally, it might happen the passive misalignment of its positions, deriving from extraneous causes to its will, that may cause unpredictable and significant changes in the net equity of the fund or on the capital market general conditions. On this situation, the Manager will obey the rules and procedures provided on the valid regulations for this kind of misalignment.

On any other misalignment situation not characterized as passive, the Manager will immediately cease any activity that might aggravate such misalignment and will adopt, immediately, actions to reduce the positions that are misaligned, with full consent of the Manager's responsible officer before the CVM, who will communicate such fact to the Compliance Officer, in such a manner as the compliance to internal or regulatory limits are again respected immediately.

After the re-establishment of the exceeded limits, the Compliance Committee shall immediately meet to discuss the reasons that led to the misalignment, to establish new procedures to avoid new occurrences and, eventually, to punish the Employee who acted in an active manner on this misalignment.

## **7. Conflict of Interests**

Conflict of Interests are situations arising from the fulfillment of certain Employee duties, on which the personal interests of this Employee might be divergent or conflicting with the Manager interests and/or among different interests of two or more of its clients, clients for whom the Manager has an obligation to each of them ("Conflict of Interests").

The Employee has the obligation to act in good faith and in accordance with the investors interests aiming at not hurting the fiduciary relation with the client. To that end, the Employee shall be alert to possible conflict of interests situation, and whenever such situation occurs, shall immediately inform, any of the Compliance Committee members about their existence and shall abstain from performing the task or omission that gave rise to the Conflict of Interests until it is otherwise decided.

## **8. Party Politics**

The Manager determines that Partners and Employees keep uninvolved to actions that may represent potential conflicts, respecting individual ideologies, but without bring them to professional environment, removing any type of connection to Manager. To link political activities to suppliers and services providers hiring is forbidden.

In addition, Partners and Employees are forbidden to practice any party-political activity within the company.



## **9. Training Policy**

The Manager possesses an initial training process for all its Employees and a continuous knowledge retraining program of such Employees, especially those that have access to confidential information or are part of investment decision processes, related to the Manager's general principles and Compliance rules described in this Policy, as well as to the principal laws and rules applicable to its activities, as included on the Appendix III of this Policy.

The Manager adopts an annual retraining program for its Employees, with the purpose of making them always up to date on the terms and responsibilities herein described, as well as on laws and rules that govern the Manager's activities, all being obliged to participate of such retraining programs and to attest in written that have understood the norms and rules transmitted.

The Compliance Committee may hire specialized professionals to conduct the initial training and retraining programs, according to the topics to be covered.

## **10. Information Security**

Information security measures have as purpose to minimize threats to the Manager's businesses and to this Policy's provisions.

Information security generally refers to: clients, suppliers and third party service providers, Partners and Employees information gathering, use, treatment and retention. By Information Treatment understands: obtaining, storing (including retention periods), sharing, accessing, and visualizing information. As regards to Information, this must be understood in a broad sense, not only classified as personal sensitive or confidential, but as those which include the company's or economic group financial information, or yet other that the company wishes to not publicize.

The recent evolution of Brazilian law has improved rules and good practices of local market by editing the LGPD (Personal Data Protection Law) and, for its compliance, internally we also have a Cybernetic Security Policy. The principles there presented must be read jointly with this Compliance Policy.

It is strictly forbidden for the Employees to make copies (physical or electronic) or to print files used, generated or available on the Manager's network and to circulate on external environments to the Manager with these files, since these files have information that are considered as confidential information. Any exception to the present rule shall be previously authorized in written by any Compliance Committee members.

The prohibition above referred does not apply when the copies (physical or electronic) or the print of files are on behalf of the execution and performance of the Manager's business and interests. On these cases, the Employee that possesses or guards the copied or printed file that has



confidential information shall be the direct responsible for its good condition, integrity, and maintenance of its confidentiality.

In consonance with the internal rules above, the Employees must abstain from using flash-drives, floppy disks, tapes, disks, or any other medium that does not have as its purpose the exclusive use for the fulfillment of her/his activity in the Manager.

The use of Manager's assets and systems, including computers, phones, internet, email, and other appliances, is destined primarily for professional purposes. The indiscriminate use of these assets and systems for personal purposes must be avoided and shall never have priority against any professional use.

Sending or forwarding by email materials that contains discriminatory, prejudiced, obscene, pornographic, or offensive content is also strictly forbidden, as well as sending or forwarding of emails with opinions, comments or messages that may denigrate the image and affect the reputation of the Manager.

Receiving emails often does not depend on the Employee him/herself, but it is expected that all have common sense to, if possible, avoid receiving messages with the content previously described. In the possible event of receiving messages with the content above mentioned, the Employee must erase them immediately, so that these remain the least possible time on the Manager's servers and computers.

Viewing websites, blogs, photologs, webmail, among others, that contain discriminatory, prejudiced (on origin, race, creed, religion, social class, political opinion, age, gender, or disability), obscene, pornographic or offensive content is strictly forbidden.

The password and login for access to the data contained in all computers, as well as on the emails that may also be accessed via webmail, must be known by the respective user of the computer and are personal and non-transferable, and shall not be disclosed to any third parties.

For the security of Employees access profiles, the Employees' access passwords are laid out according to the rules established by the Manager's IT department, as defined jointly with Risks Committee and Compliance Committee, for the implementation of the Employees' access profiles.

Aiming to increase the security level on access permission management, Manager uses double factor authentication solution to access all workstations, where even having login and password, it will be necessary to execute a second authentication level by mobile, duly configured to each employee, which is personal and non-transferable. On this manner, the Employee might also be made responsible if she/he makes available to third parties the password and login above mentioned, for any purposes.



Each Employee is yet responsible for keeping control over security of stored or made available information on the equipment of which they are in charge.

Every Employee must be conscientious on the use of their own equipment and systems and look after the good use of every other. In case some Employee identifies poor conservation, misuse or inadequate use of any other asset or systems, he/she must communicate the incident to any Compliance Committee member.

The Manager's policy is to not to make available, forward or sell any personal information that belongs to funds investors managed by itself or to which it provides investments consultancy. The Manager does not forward and shall not forward to third party providers any personal information from its investors without the respective previous and written consent, except if demanded by regulatory bodies and/or Government agencies.

## **11. Monitoring and Access Control**

The access by Employees to the Manager's premises is done through an access name badge, personal and non-transferable, and biometrics, which are made available/registered to each Employee at the moment of their hiring by the Manager.

The access to electronic information network relies on the use of exclusive Manager's servers, which cannot be shared with other companies responsible for different activities on the financial and capital market.

Considering that the use of computers, internet, email, and other devices is destined exclusively for professional purposes, as means for the performance of Employees activities, the Manager monitors the use of these resources.

On this regard, the Manager:

- (a) maintains different access levels to the folders and electronic files in accordance with the Employees' functions, and may monitor the Employees access to such folders and files on the basis of password and login made available;
- (b) may monitor the Employees access to websites, blogs, photologs, webmail, among others, as well as the emails sent and received;
- (c) may monitor the Employees phone calls, done or received through the phone lines made available by the MANAGER for the professional activity of each Employee, specially, but not limited to, phone calls to customer service team and to MANAGER operations desk.



## **12. Information Archiving**

In accordance with what is set forth on this Policy, Employees shall maintain archived each and every information, as well as documents and bank statements that might be necessary for satisfactory realization of possible audit or investigation about possible investments and/or clients suspected of corruption and/or money laundering, in conformity with clause IV of Article 16 of CVM Instruction 558, by the period of 5 (five) years or more, on the hypotheses demanded by the legislation and regulations in effect.

## **13. Anti-Money Laundering Policy and Know your Client (“KYC”)**

### **13.1. Money Laundering**

Any suspicion of financial and non-financial operations that may involve activities related to crimes of money laundering, concealment of assets and funds, as well as incorporating gains in an illicit manner, for the Manager, clients or for Employee, shall be immediately communicated to any of the Compliance Committee members, anonymously through the communication channel present on the Manager’s website.

The analysis shall be done case by case, the responsible being subjected to the sanctions foreseen on this Policy.

Beyond a thorough process of selection of brokers (intermediaries) with which intends to engage with, the Manager must establish an identification process of adequate counterparts to the characteristics and particularities of the business that intends to perform. Such process aims to prevent that the counterpart, when identifiable, uses the investment funds or securities portfolios managed for illegal or improper activities.

The assets and shares listed here below, due to their counterpart and of the market on which are negotiated, have passed through a verification process, nevertheless, the Manager will always endeavor on the identification process of the counterpart, in case such endeavor is possible in reason of the circumstances and characteristics of the asset to be invested on, namely: (a) securities initial and secondary public offers, registered in accordance with the norms issued by CVM; (b) restricted efforts public offers, exempt of register in accordance with the rules emitted by CVM; (c) assets and stocks admitted for negotiation in stock exchange, commodities and futures markets, or registered in a registration, custody or financial settlement system, duly authorized in their countries of origin and overseen by recognized local authority; (d) assets and stocks whose counterpart is a financial institution or similar; and (e) assets and stocks of the same economic nature of those listed above, when negotiated abroad, as long as (i) are admitted to negotiation in stock exchange, commodities and futures markets, or duly authorized or registered on registration, custody or financial settlement system duly authorized on their countries of origin





and overseen by local authority recognized by CVM, or (ii) the existence of which was assured by third party duly authorized for the exercise of the activity of custody in countries signatory of the Treaty of Asunción or in other jurisdictions, or overseen by local authority recognized by CVM.

For the other assets and securities, such as stocks and bonds which are object of private distribution (fixed income or stocks), receivables, real estate ventures, etc., the Manager will seek, beyond procedures of Counterparts Identification, to adopt also other procedures (such as verification visit) and internal controls, or to verify if the counterpart possesses minimal mechanisms of analysis for money laundering prevention and combat.

It is the competence of the management department and, specifically, to the Employees involved with the management, to previously inform the Compliance Officer whenever it is intended to perform an operation with the characteristics above described, so that due diligence is adopted.

Additionally, the Manager must adopt procedures aiming to control and monitor the price range of the assets and securities negotiated for the investment funds and portfolios under its management, whenever the transaction counterpart is known, in a manner so that possible operations done outside the standards exercised on the market, according to the characteristics of the business, are identified and, if the case requires, communicated to the competent bodies.

### **13.2. COAF Communication**

The situations listed below in a non-exhaustive manner might constitute indications of crimes occurrence described in the Law No. 9.613, or may be related to them, having to be analyzed with special attention, and, if and when considered suspect by Employees, on the terms of ICVM 617, communicated to COAF (Control Board of Financial Activities):

- a) perform operations, or operations group of purchase or sale of assets and stocks to the fund, that present themselves untypical in relation to the counterpart's economic activity, as long as it is known;
- b) resist to supply the necessary information for development of regular course of business, giving false information or information of difficult or onerous verification;
- c) present irregularities related to identification and register procedures of operations demanded by the valid regulations;
- d) request of non-compliance or acting in a way as to induce institution employees to not follow the statutory or formal procedures to perform operations or operations group of purchase or of sale of assets and stocks to the fund; or
- e) any operation or operations group of purchase and sale of securities with signs of terrorist



financing.

The analyses conclusions registers regarding operations or proposals that substantiated the decision of performing, or not, the communications that the above paragraph addresses, must be kept by the period of 5 (five) years, or by a longer period by express resolution of CVM, in case of administrative process.

### **13.3. Know Your Client**

The client's information possibly collected by the Manager jointly with the funds administrator managed by the Manager ("Administrator") must be in accordance with the global and local procedures of Money Laundering Prevention Terrorism Financing Combat according to what is described on this Policy.

The Manager will count on the efforts of administrators, distributors and custodians of the funds that are or may come to be managed by it to (i) identify new or already existent clients, including previously to the effective performance of the investments; and (ii) prevent, detect, and report any suspicious operations.

Regardless of the special process of "Know Your Client" applicable to these Clients categories, the acceptance of PEP as client to the Manager on the services provided by it always rests on the authorization of the Manager's administrators.

### **14. Anticorruption Policy**

Law 12.846/13 characterized the objective liability of legal entities in case of involvement in corruption acts and brings strict sanctions and penalties for those who violate the law. All the Employees of the manager must observe, obey and make comply with the terms and conditions of Law and this Policy, without damage to the related legislation. For the purposes of this Policy, it will not be tolerated any form of Corruption.

The Employees are forbidden to engage in the following conducts:

- (i) to promise, offer or give, directly or indirectly, undue advantage to Public Agent, or to third party to them related;
- (ii) finance, fund, sponsor or in any way endorse the practice of illicit acts foreseen in the Anticorruption Law;
- (iii) to make use of physical or legal intermediary person to occult or dissimulate your real interests or the identity of the beneficiary who did the act;
- (iv) to hamper investigation or inspection activities of bodies, entities or Public Agents, or intervene in their action, including in the scope of regulatory agencies and national financial



system inspection bodies.

Moreover, regarding participation in bidding and signing of administrative contracts, it is forbidden to the Employees:

- (i) to frustrate or fraud, by means of tampering, manipulation, or any other expedient, the competitive character of the public bidding procedure;
- (ii) impede, perturb or fraud the performance of any act of public bidding procedure;
- (iii) to move away or to attempt to move away any bidder, by means of fraud or the offering of any kind of advantage;
- (iv) to fraud public bidding or contract resulting from it;
- (v) to create, by fraudulent or irregular means, legal entity to take part in public bidding or to celebrate administrative contract;
- (vi) to obtain advantage or undue profit, in a fraudulent manner, of modifications or renewals of contracts signed with Governmental body without lawful authorization, on the invitation of public bidding or on the respective contractual instruments;
- (vii) to manipulate or fraud the economic financial equilibrium of the contracts signed with a Governmental body.

## **15. Advantages, Benefits and Gifts**

Employees shall not, directly or indirectly, neither for themselves nor for third parties, request, accept or admit money, benefits, favors, gifts, promises or any other advantages in equivalent value over to R\$1,000.00 (one thousand reais) by client, that may influence the performance of their functions or as recompense for act or omission resulting from their work, except on the hypotheses and conditions foreseen on this Policy, the case being that the compliance to this shall be declared by the Employee when signing the Engagement Letter annexed to this document.

## **16. Soft Dollar**

In general terms, *Soft Dollar* can be defined as being the economic benefit, of non-pecuniary nature, possibly granted to resource managing entities by securities brokers or other suppliers ("Suppliers"), in remuneration to the directing of investment funds transactions managed by the resource managing entities.

In case such agreements are made, all benefits shall be reverted to the investment funds and portfolio under management of the Manager.

In case of doubt, the Compliance Officer shall be consulted.



Such benefits shall be utilized by the Employees exclusively for purposes of investment decision-making and support to the management of stock portfolios managed by the Manager.

The Manager shall not select its Suppliers considering only the benefits received through such agreements of *Soft Dollar*, but will take into account, primarily, the quality, efficiency, productivity and the costs offered by such Suppliers.

The Manager, through its representatives, shall observe the following principles and rules of conduct when signing *Soft Dollar* agreements:

- a) to put the interests of the clients above its own interests;
- b) define in good faith if the values paid by the clients and, consequently, passed on to the Suppliers, are reasonable in relation to the orders execution services;
- c) to be certain that the *Soft Dollar* benefit will immediately abet in the process of investment decision-making and allocate the costs of the service received in accordance with its use, if the benefit presents a mixed nature;
- d) to broadly diffuse to clients, potential clients and the market, the criteria and policies adopted in relation to the *Soft Dollar* practices, as well as the potential conflicts of interests deriving from the adoption of such practices;
- e) to fulfill with its duty of loyalty, transparency, and fidelity with the clients; and
- f) to transfer to the clients' portfolio any benefits or advantage that might come to have due to its condition of manager of securities portfolio, in agreement with Article 16, clause VI of the CVM Instruction 558/15.

*Soft Dollar* agreements must be transparent and kept in written documents with acknowledgement of the Compliance Officer.

By hiring the services of orders execution, the Manager shall not only look for the lower cost, but to best cost-benefit, in alignment with the best execution criteria laid down in the international market, having to be capable of justifying and proving that the values paid to the Suppliers with whom has hired *Soft Dollar* are favorable to the securities portfolio under its management in comparison to other Suppliers, considering not only the related costs, but also the quality of the services offered, which comprehend better efficiency in transactions execution, security conditions, better negotiations platforms, distinctive customer service, supply of stock analysis services and technical quality of corresponding materials, availability of IT systems, among others.

Any benefits unrelated to the investment decision-making process, such as the payment of office expenses, travels, entertainment, among others, must not be the object of *Soft Dollar*.

*Soft Dollar* agreements must not generate any arrangement of exclusivity or the duty of execution



of a minimal volume of transactions with the Suppliers, the Manager being obliged to keep at all times total independence to select and realize with any Suppliers operations on behalf of the securities portfolios under management, always in pursuit of the best conditions for its clients.

## **17. Third Party Hiring Policy**

For the present Third Party Hiring Policy, it is considered third party any person, individual company, business society or similar that provides products or services of any nature to the Manager (“Third Party”).

### **17.1. Procedures**

After being hired, it is the duty of Employees to accompany the Third Party’s services, having to be always attentive to eventual warning signals or of non-compliance to the regulations but not limited to, the Law No. 12.846/13 (Anticorruption Law). The Third Parties contracts shall be reassessed annually by the Partners, through a coordinated process by the Compliance Officer that will rely on the help of other Employees, according to the use of the respective services utilized by each Employee.

If, on the case of described above verifications, before or after hiring products and services by the Manager, it is attested that a Third Party potentially offends the provisions of this Third Party Hiring Policy, the Compliance Committee shall analyze the case and decide on the hiring or continuation of the products and services, as the case requires.

In case of any type of connection between a service provider with one of the Employees, the hiring shall be approved by the Compliance Officer through a document where the nature of the connection between the mentioned service provider and the Employee shall be detailed, confirming that she/he believes that the connection will not cause the violation of rules or any damage to the Manager, including its reputation.

### **17.2. Brokers Hiring**

In addition to the procedures described above, the selection and hiring of brokers for the execution of orders for securities portfolios under the management of the Manager shall take into account, mainly, the following aspects:

- a) service quality;
- b) availability;
- c) price; and



d) quality of the research provided, in case of research brokers.

The brokers approval shall be analyzed by the Risk Committee.

### **17.3. Back-Office Hiring**

Beyond the described above procedures, in case the Manager hires a Third Party for the providing back-office services and stock analysis, it shall adopt rules and internal procedures capable of assuring the complete segregation of functions, activities and responsibilities related to the activity of resource management.

In this case, all Employees that have their professional activities related to resource management will be allocated in a separate site from the other third-party services providers, including exclusive access by means of electronic control systems, the use of physical facilities totally independent and segregated, made available specific phone lines and private and restricted directory, accessible only through personal login and password.



## APPENDIX I - ENGAGEMENT LETTER

By means of this instrument, I, \_\_\_\_\_, enrolled in Individual Taxpayer Register (CPF/MF) under No. \_\_\_\_\_, declare for all due purposes, that:

1. Am aware that what is provided in the Ethics Code, Compliance Policy (*June 2024 version*), Personal Investment Policy, Risk Management Policy, and Securities Portfolios Orders Proration and Division Policy of **Dunamis Trading Gestão de Recursos Ltda.** (“Manager”), will come to be part of my duties as a Manager’s Employee, along with what is provided in the Confidentiality Agreement.
2. Commit myself to report immediately to the Manager any fact that I may come to be aware of that may present any risk to the Manager.
3. From this date onwards, the non-compliance of the Confidentiality Agreement and/or of this Engagement Letter may imply being characterized a serious misconduct, a fact that might be liable to the application of foreseen penalties, including as a consequence the employment agreement termination, when applicable, or dismissal, or exclusion, applied to my function at the time of the fact, obliging me to compensate the Manager and/or third parties for the eventual losses, damages or harm and/or loss of profits, regardless of the adoption of the applicable legal measures.
4. The rules stated in the Confidentiality Agreement and on the Engagement Letter do not invalidate any societal clause, of the employment agreement, nor of any other rule set forth by the Manager, but only serve as support and clarify on how to handle certain situations related to my professional activity. I am aware they are prohibited.
5. Am aware that it is strictly forbidden any personal investment by Employees and Related Parties in securities that are part of the listing of managed portfolios and/or of investment funds managed by the Manager, unless expressly authorized by the Compliance Committee.
6. Have taken part on the Manager initial training, where I was made aware of the principles and rules applicable to my and the Manager’s activities and had the opportunity to clarify doubts related to such principles and rules, so that I have understood them, and commit myself to observe them in the fulfillment of my activities, as well as to participate assiduously in the continuous training program.
7. Am aware that it is strictly forbidden to make copies (physical or electronic) or to print the files used, generated or available on the Manager’s network and to circulate on external environments to the Manager with these files without due authorization, since such files contain information that are considered confidential information, as described in the Confidentiality



Agreement.

8 Am aware that the Manager might record any phone calls done or received through the phone lines made available by the Manager for my professional activity, specially, but not limited to, the calls of the customer service team and the Manager's operations desk.

9 Am aware that the Manager monitors all and every exchange, internal or external, of my email, as well as my access to websites and electronic files.

10 Am aware that the login and password for the access to the data contained in all computers, including emails, are personal and non-transferable, so that I commit to not disclose them to other Manager's Employees and/or any third parties.

11 Am aware that I shall not, direct or indirectly, neither for myself nor for third parties, request, accept or admit money, benefits, rewards, gifts, promises or any other advantages that might influence the performance of my functions or as a reward for any act or omission deriving from my work.

São Paulo, [\*] [\*], [\*]

---

[EMPLOYEE]





## APPENDIX II - CONFIDENTIALITY AGREEMENT

By means of this instrument, I, \_\_\_\_\_, enrolled in Individual Taxpayer Register (CPF/MF) under No. \_\_\_\_\_, henceforth denominated Employee, and **Dunamis Trading Gestão de Recursos Ltda.** (“Manager”).

The parties decide, for the purpose of safekeeping of personal and professional information of the clients and the MANAGER, to sign this confidentiality agreement (“Agreement”), that shall be ruled by the clauses here presented:

1. For the purposes of this Agreement, are considered confidential information (“Confidential Information”) regardless of this information being contained in disks, floppy disks, flash-drives, tapes, other kinds of medium or in physical documents, or being written, verbal or presented in a tangible or intangible manner, any information about the Manager, its partners and clients including:

- a) know-how, techniques, copies, diagrams, models, samples, computer software and network infrastructure;
- b) technical, financial, or related information to investment and divestment strategies or trading; including balances, bank statements and clients’ investment funds and portfolios positions managed by the Manager;
- c) structured operations, other operations and their respective values, analyzed or performed by investment funds and portfolios managed by the Manager;
- d) reports, studies, internal opinions on financial assets;
- e) clients list, commercial counterparts, suppliers and service providers;
- f) strategic or market information, or of any nature related to the Manager’s and its clients or partners activities;
- g) information regarding financial results previous to publication of balances, trial balances and/or financial statements of the investment funds and portfolios managed by the Manager;
- h) transactions performed and which have not yet been published; and
- i) other information obtained with Manager’s partners, officers, employees, trainees, interns or “young apprentices”, or yet, with their representatives, consultants, advisors, clients, suppliers, and service providers in general.

2. The Employee commits her/himself to use Confidential Information to which it may have access to, strictly and exclusively for the performance of her/his activities within the Manager, committing her/himself, therefore, to not disclose such Confidential Information for any purposes, unauthorized Employees, media, or outsiders to the Manager, including, in this last case, spouse, companion, ascendant or descendant, any person of close relationship or financially dependent of the Employee.



2.1 The Employee obliges to, during the duration of this Agreement and for an undefined period after its termination, to keep absolute personal and professional secrecy of the Confidential Information to which has had access during her/his work period at the Manager, being yet committed to not use, practice, or disclose privileged information, Insider Trading, Privileged Disclosure and Front Running, be it on her/his own behalf, of the Manager, or of third parties.

2.2 The nonobservance of confidentiality and secrecy, even after this Agreement end of term, will be liable on civil and criminal spheres.

3 The Employee understands that the unauthorized disclosure of any Confidential Information may cause irreparable damages without legal remedy to the Manager and third parties, being the Employee from now on obliged to compensate the Manager, its partners and third parties damaged, in the terms set forth below.

3.1 The non-compliance above described will be considered civil and criminal violation, resulting also on the termination of the employment agreement, when applicable.

3.2 The Employee is aware that will be responsible to prove that the inadequately disclosed information is not Confidential Information.

4. The Employee acknowledges and is aware that:

a) All the documents directly or indirectly related to the Confidential Information, including contracts, contract drafts, letters, facsimiles, presentations made to clients, emails and all types of electronic correspondence, files and computerized systems, spreadsheets, action plans, evaluation models, analyses, management and memos composed by her/him, or obtained due to the performance of activities at the Manager are and will remain exclusive property of the Manager and its partners, in reason of which she/he commits to not make use of such documents, at present or in the future, for any purposes other than the fulfillment of her/his activities at the Manager, being mandatory that all documents remain under guardianship and custody of the Manager, unless if in virtue of the Manager's interests is necessary for the Employee to keep such documents or their copies outside the Manager's premises;

b) In case of termination of the individual employment agreement, discontinuation or exclusion of the Employee, the Employee shall immediately give back to the Manager all documents and copies that have Confidential Information that are in her/his possession;

c) By the terms of Law 9.609/98, databases, internally developed computerized systems, computerized models of analysis, evaluation and management of any nature, as well as electronic files, are of exclusive property of the Manager, being expressly forbidden their total or partial reproduction, by any means or processes; its translation, adaptation, reordering or any other modification; to distribution of the original or copies of the database or its disclosure to the public; reproduction, distribution or communication to the public of partial information, of operations results related to the database, or yet, spread of rumors, the Employee is subject, in case of infringement, to the penalties stated on the mentioned law.

5. On the hypothesis of the Employee be requested, by Brazilian or foreign authorities (in



oral questions, interrogations, requests of information or documents, notifications, indictment or warrant, and investigations of any nature) to divulge any Confidential Information to which has had access, the Employee shall immediately notify the Manager, so as to allow the Manager to pursue the pertinent legal measure to attend or avoid the disclosure.

5.1 In case the Manager does not obtain the legal order to prevent the information disclosure in a timely manner, the Employee may provide the Confidential Information requested by the authority.

In this case, giving the Confidential Information requested shall be restricted exclusively to that which the Employee is obliged to disclose.

5.2 The duty of notifying the Manager subsists even after the individual employment agreement is terminated, or the Employee is dismissed or excluded, by an indeterminate period.

6. This Agreement is an integral part of the rules that govern the work and/or societal relation of the Employee to the Manager, who by signing it is expressly accepting the terms and conditions herein affirmed.

6.1 The transgression of any of the rules described in this Agreement, without prejudice to what was provided on item 3 and subsequent ones above, will be considered contractual breach, subjecting the Employee to the sanctions that are attributed by the Manager's partners.

Thus, being in accord with the conditions mentioned above, sign this in 02 (two) copies of equal content and form, to produce a singular effect, on the presence of the witnesses signed below.

São Paulo, [\*] [\*], [\*]

---

**[EMPLOYEE]**

---

**Dunamis Trading Resource Management Ltd.**

Witnesses:

1. \_\_\_\_\_

Name:

Individual Taxpayer Register (CPF):

2. \_\_\_\_\_

Name:

Individual Taxpayer Register (CPF):



## APPENDIX III - MAIN REGULATIONS

1. CVM Instruction No. 558/15
2. CVM Instruction No. 555/14
3. CVM Instruction No. 617/20
4. CVM/SIN Circular Memorandum No. 05/2014
5. Money Laundering and Terrorism Funding Prevention Guide of the Brazilian Capital Market, elaborated by ANBIMA
6. ANBIMA Regulation and Best Practices for Investment Funds Code
7. ANBIMA Accreditation Code
8. Law 9.613/98, as altered

**Reference Date: June, 2024**<sup>1</sup>

**1 Attention:** All Collaborators must check the term and possible amendments to the regulations contained in this Appendix previous to their use.